

REMARKS

The present application was filed on May 20, 1999 with claims 1-27. Claims 1-27 are currently pending in the application. Claims 1, 11 and 22-27 are the independent claims.

Applicant initially notes that claim 24 is both allowed (Office Action, p. 8) and rejected under 35 U.S.C. §102(e) as being anticipated by Mathematica: A System for Doing Mathematics by Computer, First Edition by Wolfram (hereinafter “Wolfram”) (Office Action, pp. 5-6). This contradiction makes it impossible for the Applicant to be fully responsive to the present Office Action with respect to this claim, as required by 37 C.F.R. §1.111. Applicant, therefore, submits that the Office Action is improper with respect to claim 24, and that any subsequent Office Action that rejects claim 24 should, as a result, be made non-final.

In the present Office Action, claims 1-10, 22, 23, 25 and 27 are rejected under 35 U.S.C. §101 as being directed to non-statutory subject matter. Moreover, claim 17 is rejected under 35 U.S.C. §112 for insufficient antecedent basis. Claims 1, 2, 6, 11, 12, 16, 22 and 25-27 are rejected under 35 U.S.C. §102(b) as being anticipated by “Disavowal protocol for Chaum-van Antwerpen undeniable signature scheme” described in Handbook of Applied Cryptography by Menezes (hereinafter “Menezes”). Claim 24 is rejected under 35 U.S.C. §102(e) over Wolfram. In addition, claims 3 and 13 are rejected under 35 U.S.C. §103(a) as being unpatentable over Menezes. Furthermore, claims 10 and 20 are rejected under 35 U.S.C. §103(a) as being unpatentable over Menezes in view of “Distributed Provers with Applications to Undeniable Signatures” by Pedersen (hereinafter “Pedersen”). Finally, claim 21 is rejected under 35 U.S.C. §103(a) as being unpatentable over Menezes in view of Pedersen, in further view of Computer Architecture: A Quantitative Approach, Second Edition by Patterson and Hennessey.

Claims 14, 15 and 17-19 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form.

With respect to the §101 and §112 rejections of claims 1-10, 22, 23, 25 and 27, Applicant chooses to amend the independent claims in order to address the Examiner’s concerns. Applicant, therefore, respectfully requests that the Examiner reevaluate these claims, as amended, in light of the following comments.

In formulating the §101 rejection of claims 1, 23 and 25, the Examiner states that “the claimed subject matter is a process that only manipulates abstract ideas or concepts” and that “[n]othing in the claim language suggests a dependence on a computer system, distinguishing the claimed method from a ‘pencil and paper’ method” (Office Action, p. 3). In response to this rejection, Applicant chooses to amend these claims so that the methods described are “being implemented in a digital data processor including a processor and a memory.” These amendments are supported in the specification and drawings, as originally filed, e.g., p. 5, lines 20-26 and FIG. 1. Applicant submits that these additional limitations put the independent claims in condition for allowance over the §101 rejection. Applicant further submits that dependent claims 2-10 are also put into condition for allowance by the amendment to claim 1.

With respect to the §101 and §112 rejections of claim 17, the Examiner states that the claim “falls under two statutory classes as both an apparatus and method are claimed” and is “indefinite because reference to ‘the method’, line 3 does not further limit the apparatus claim 11 (*sic*)” (Office Action pp. 3-4). Accordingly, Applicant chooses to amend this claim so that it no longer describes both an apparatus and a method. As amended, the claim describes only an apparatus.

Finally, in formulating the §101 rejection of claims 22 and 27, the Examiner states that “the claimed subject matter is embodied on a computer-readable medium; however, the method steps claimed are directed to non-statutory subject matter and are directed to software *per se*” (Office Action, p. 3). In response, Applicant notes that the Manual of Patent Examination, Eighth Edition, August 2001 (MPEP) §2106 specifies that a computer-related process may be statutory if “it is limited to a practical application within the technological arts.” Moreover, §2106 states that “[a] claim is limited to a practical application when the method, as claimed, produces a concrete, tangible and useful result.” In light of these requirements, Applicant chooses to amend claims 22 and 27 such that the claimed programs on the computer-readable medium implement “a cryptographic protocol between multiple parties comprising a prover and a verifier” and a result of a claimed step or operation is “utilizable in implementing the cryptographic protocol.” These amendments are supported in the specification and drawings, as originally filed, e.g., p. 8, line 25 to p. 9, line 2, and

FIGS. 2 and 5. Applicant respectfully submits that these added limitations provide the practical application required under §101 and, thereby, put these claims in condition for allowance.

With respect to the §102(b) and §102(e) rejections, Applicant initially notes that MPEP §2131 specifies that a given claim is anticipated “only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference,” citing Verdegaal Bros. v. Union Oil Co. of California, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). Moreover, MPEP §2131 indicates that the cited reference must show the “identical invention . . . in as complete detail as is contained in the . . . claim,” citing Richardson v. Suzuki Motor Co., 868 F.2d 1226, 1236, 9 USPQ2d 1913, 1920 (Fed. Cir. 1989).

With respect to the §102(b) rejection of independent claims 1, 11, 22 and 25-27 as being anticipated by Menezes, Applicant continues to traverse the Examiner’s rejection for the same reasons articulated by the Applicant in the response to the first Office Action. Nonetheless, despite this traversal, Applicant chooses to amend the claims without prejudice to better clarify the scope of the invention. In formulating the §102(b) rejections of claims 1, 11, 22 and 25-27, the Examiner argues in the Office Action on p. 2:

On page 477, Menezes discloses a proof of a proof. The signature is already created. By concluding a disavowal, B is proving whether A has correctly proved the validity of the signature. In step 3, A is performing a proof. In step 8, B is proving the correctness of A’s proof.

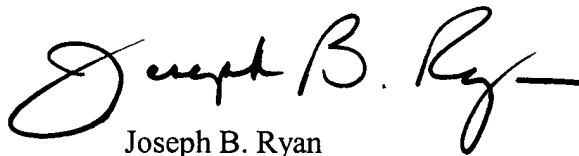
In light of these comments, Applicant chooses to modify the claims so that it is clear that the two verifying proofs described in the claims are both performed by the prover. These amendments are supported in the specification and drawings, as originally filed, e.g., p. 8, lines 17-24 and FIG. 2. In contrast, Applicant notes that, in Menezes, “A” is the signer and “B” is an entity that wishes to verify this signature (see Menezes, p. 476, section 11.122). As a result, Menezes describes a process in which two separate entities perform proofs. Menezes, therefore, does not describe each and every element of the amended independent claims.

Accordingly, Applicant respectfully submits that independent claims 1, 11, 22 and 25-27, as amended, are in condition for allowance. Dependent claims 2, 6, 12 and 16 are also believed allowable for at least the reasons identified above with regard to their respective independent claims and are further believed to contain separately patentable subject matter relative to Menezes and other prior art of record.

Finally, with respect to the §103(a) rejections of claims 3, 10, 13, 20 and 21, Applicant respectfully submits that the proposed reference combinations fail to supplement the above-described fundamental deficiencies of Menezes as applied to independent claims 1 and 11. Therefore, the subject matter as a whole of dependent claims 3, 10, 13, 20 and 21 would not have been obvious at the time the invention was made and should be allowed.

In view of the above, Applicant submits that claims 1-27, as amended, are in condition for allowance. Applicant respectfully requests the withdrawal of the §§ 101, 112, 102(b) and 103(a) rejections with respect to the claims.

Respectfully submitted,

A handwritten signature in black ink, appearing to read "Joseph B. Ryan", with a long horizontal stroke extending to the right.

Date: September 22, 2004

Joseph B. Ryan
Attorney for Applicant(s)
Reg. No. 37,922
Ryan, Mason & Lewis, LLP
90 Forest Avenue
Locust Valley, NY 11560
(516) 759-7517